*N.C.* On page 10, line 11, after "110a-110d" delete -- itself --

On page 15, line 08, replace "whether the servlet" with -- whether a servlet --

On page 16, line 11, replace "is" with -- can also be --

On page 24, line 09, replace "110a-110d ." with -- 110a-110d. --

On page 24, line 17, replace "negotiate" with -- negotiates --

In the Claims:

(For the convenience of the Examiner, all pending claims are provided; all claims amended herein are marked with a preceding double asterisk, "**").

Please amend the *EXISTING* claims as follows.

** 1. (Three times amended) A system on a server computer system, comprising:

a communications engine for establishing a communications link with a client;

security services coupled to the communications engine for determining client privileges;

a web server for enabling the client to select a service from a set of available services, the set of available services based on the client privileges;

a host engine coupled to the security services and to the web server for providing to the client service communication code that enables communication with a selected service; and

a keysafe for storing keys, each key for enabling communication between the client and a respective service from the set of available services, thereby enabling the client to access the available services without storing the service communication code and keys at the client.

2. (Once amended) The system of claim 1, wherein the communications engine uses SSL to create a secure communications link with the client.

3. The system of claim 1, wherein communications engine negotiates an encryption protocol for transferring messages to and from the client.

4. The system of claim 1, wherein the communications engine uses public key certificates for transferring messages to and from the client.

5. (Twice amended) The system of claim 1, wherein the security services use public key certificates to authenticate a user of the client to determine the client privileges.

6. (Twice amended) The system of claim 1, wherein the security services examine the identity of a user of the client and the level of authentication to determine the client privileges.

7. (Twice amended) The system of claim 1, wherein the security services examine a public key certificate to authenticate the client to determine the client privileges.

8. (Twice amended) The system of claim 1, wherein the security services use a digital signature to authenticate the client to determine the client privileges.

9. (Twice amended) The system of claim 1, wherein the [servlet] host engine forwards to the client security code for enabling the client to perform a security protocol recognized by the security services.

10. (Twice amended) The system of claim 1, wherein one of the available services is secured by a firewall and one of the keys is configured to enable communication through the firewall.

11. (Once amended) The system of claim 1, further comprising a firewall for protecting the system.

12. (Twice amended) The system of claim 1, wherein one of the keys includes an address identifying the location of the selected service.

13. (Twice amended) The system of claim 1, wherein the code uses a key to provide to the client a direct connection with the selected service.

14. (Twice amended) The system of claim 1, further comprising a proxy for communicating with the selected service, and wherein the code enables the client to communicate with the proxy and one of the keys enables the proxy to locate the selected service.

** 15. (Three times amended) A computer-based method comprising:

establishing a communications link with a client;

determining client privileges;

enabling the client to select a service from a set of available services, the set of available services based on the client privileges;

providing to the client <u>service communication</u> code that enables communication with a selected service; and

retrieving a key from a set of keys, each key corresponding to a respective service from the set of available services, the retrieved key for enabling communication between the client and the selected service<u>, thereby enabling the client to access the available services without storing the service communication code and keys at the client</u>.

16. (Once amended) The method of claim 15, wherein establishing a communications link includes the step of using SSL to create a secure communications link with the client.

17. The method of claim 15, wherein establishing a communications link includes the step of negotiating an encryption protocol for transferring messages to and from the client.

18. The method of claim 15, wherein establishing a communications link includes the step of using public key certificates for transferring messages to and from the client.

19. (Once amended) The method of claim 15, wherein determining client privileges includes the step of using public key certificates to authenticate a user of the client.

20. (Once amended) The method of claim 15, wherein determining client privileges includes the step of examining the identity of a user of the client and the level of authentication.

21. (Once amended) The method of claim 15, wherein determining client privileges includes the step of examining a public key certificate to authenticate the client.

22. (Once amended) The method of claim 15, wherein determining client privileges includes the step of using a digital signature to authenticate the client.

23. (Once amended) The method of claim 15, wherein establishing a communications link includes forwarding to the client security code for enabling the client to perform a recognized security protocol.

24. (Twice amended) The method of claim 15, further comprising the step of using one of the keys to communicate through a firewall to the selected service.

25. (Once amended) The method of claim 15, wherein the method is performed by a server and further comprising using a firewall to protect the server.

26. (Twice amended) The method of claim 15, wherein one of the keys includes an address identifying the location of the selected service.

27. (Once amended) The method of claim 15, wherein providing includes the step of providing to the client a direct connection with the service.

28. (Twice amended) The method of claim 15, further comprising using a proxy to communicate with the service, and wherein providing includes enabling the client to communicate with the proxy.

** 29. (Three times amended) A system on a server computer system, comprising:

means for establishing a communications link with a client;

means for determining client privileges;

means for enabling the client to select a service from a set of available services, the set of available services based on the client privileges;

means for providing to the client service communication code that enables communication with a selected service; and

means for retrieving a key from a set of keys, each key corresponding to a respective service from the set of available services, the retrieved key for enabling communication between the client and the selected service, thereby enabling the client to access the available services without storing the service communication code and keys at the client.

** 30. (Three times amended) A computer-based storage medium storing a program for causing a computer to perform the steps of:

establishing a communications link with a client;

determining client privileges;

enabling the client to select a service from a set of available services, the set of available services based on the client privileges;

providing to the client service communication code that enables communication with a selected service; and

retrieving a key from a set of keys, each key corresponding to a respective service from the set of available services, the retrieved key for enabling communication between the client and the selected service, thereby enabling the client to access the available services without storing the service communication code and keys at the client.